UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/782,309	02/19/2004	Ari Juels	4414-35	7635

7590 03/21/2008

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
BANGACHON, WILLIAM L	

ART UNIT	PAPER NUMBER
2612	

MAIL DATE	DELIVERY MODE
03/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte ARI JUELS

Appeal 2007-2357
Application 10/782,309
Technology Center 2600

Decided: March 21, 2008

Before JOSEPH L. DIXON, LANCE LEONARD BARRY, and HOWARD B. BLANKENSHIP, *Administrative Patent Judges*.

DIXON, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the Examiner's final rejection of claims 1-7, 9-16, 20, 23-27, and 29-33. Claims 8, 17-19, 21, 22, and 28 are objected to by the Examiner as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

BACKGROUND

Appellant's invention relates to low-complexity cryptographic techniques for use with radio frequency identification devices (Spec. 1). An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below.

> 1. A method for use in an RFID system comprising at least one RFID device and at least one reader which communicates with the RFID device, the method comprising the steps of:
>
> associating a plurality of pseudonyms with the RFID device; and
>
> transmitting from the RFID device different ones of the pseudonyms in response to different reader queries of the RFID device;
>
> wherein an authorized verifier is able to determine that the different transmitted pseudonyms are associated with the same RFID device.

PRIOR ART

The prior art references of record relied upon by the Examiner in rejecting the appealed claims:

Dannhaeuser	US 4,928,098	May 22, 1990
Furuta	US 6,225,889 B1	May 1, 2001
Turner	US 6,724,895 B1	Apr. 20, 2004
Hughes	US 6,842,106 B2	Jan. 11, 2005

REJECTIONS

Claims 1, 2, 4-7, 20, 23-25, 30, 32, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes in view of Dannhaeuser.

Claims 3 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes in view of Dannhaeuser, and further in view of Turner.

Claims 9-13, 14-16, 26-27, and 29, are rejected under 35 U.S.C. 103(a) as being unpatentable over Hughes in view of Dannhaeuser, and further in view of Furuta.

Rather than reiterate the conflicting viewpoints advanced by the Examiner and Appellant regarding the above-noted rejection, we make reference to the Examiner's Answer (mailed April 5, 2006) for the reasoning in support of the rejections, and to Appellant's Brief (filed January 12, 2006) and Reply Brief (filed June 8, 2006) for the arguments thereagainst.

OPINION

In reaching our decision in this appeal, we have given careful consideration to Appellant's Specification and claims, to the applied prior art references, and to the respective positions articulated by Appellant and the Examiner. As a consequence of our review, we make the determinations that follow.

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988). In so doing, the Examiner must make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). "[T]he Examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability." *In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992). Furthermore, "'there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness' . . . [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007)(quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

In the Answer, the Examiner has set forth a proper initial showing at pages 4-6 and corresponding responses to Appellant's arguments at pages 11-17. The Examiner maintains that Hughes teaches all the limitations of independent claim 1 but for transmitting of different ones of the pseudonyms and relies upon the teachings of Dannhaeuser to teach and fairly suggest the use of a plurality of pseudonyms in algorithmic or tabular form (Ans. 5). The Examiner has identified the teachings in columns 5-7, of Hughes to teach associating a plurality of pseudonyms with the RFID device and identifies the use of multiple secret key values 66, 68. We agree with the

Examiner and specifically agree with the access challenge/response process as referenced at pages 5 and 19 of the Answer which uses the secret key in a process using plural pseudonyms in identifying RFID devices.

Here, the Examiner has relied upon the teachings of Dannhaeuser to teach the storing of a plurality of pseudonyms and the use thereof in combination with the teachings of Hughes to increase the security to a wireless communication (Ans. 6). We find the Examiner's position as expressed in the Answer to be reasonable in light of the teachings of Hughes and Dannhaeuser. Therefore, we look to Appellant's Brief and Reply Brief for persuasive arguments or showing of error in the Examiner's initial showing.

With respect to independent claim 1 (and independent claims 30, 32, and 33), Appellant argues that the combination results in an arrangement in which the RFID device can be authenticated without the need for complex cryptographic operations (App. Br. 4-5). We find no support in the language of independent claim 1 to distinguish between the use of various cryptographic operations. Therefore, Appellant's argument is not persuasive.

Appellant argues that the use of the secret key 66 cannot reasonably be construed as comprising a plurality of pseudonyms, or even a single pseudonym (App. Br. 4). Appellant argues that the term pseudonym as used in the present specification and in standard usage implies some ability to identify a particular entity with which the pseudonym is associated (App. Br. 4-5). Appellant argues that the secret key value itself does not provide any

device-identifying information whatsoever, and accordingly is not a pseudonym for the device. Appellant argues that Hughes teaches the use of a conventional identification code to identify a particular tag to a reader and Appellant relies upon the teachings in Hughes at column 5, lines 7-8 and 21-23. While we agree with Appellant concerning this teaching in Hughes, we note that it appears to be different than how the Examiner applied the prior art teachings of Hughes. Therefore, Appellant's argument does not correspond to the instant rejection by the Examiner and is therefore not persuasive.

In this prosecution, the Examiner has relied upon the use of the secret key value 66 or 68 and has identified the Access Challenge and Challenge Response as part of the process to identify the RFID device. Here, we agree with the Examiner's application of the prior art teachings.

Appellant argues that the secret key value 66 is not transmitted by any of the RFID devices (App. Br. 5). Here, the Examiner does not rely upon the transmission of the specific secret key, but relies upon the teachings of Dannhaeuser concerning a sequence of code words (from a table or from an algorithm) from a transmitter. Therefore, Appellant's argument does not address the rejection as applied by the Examiner. Therefore, Appellant's argument is not persuasive of error in the Examiner's initial showing.

Appellant argues that the remote keyless entry codes of Dannhaeuser do not constitute pseudonyms as claimed, because the codes do not provide any ability to uniquely identify a particular code transmitting device (App. Br. 5-6). Here, we do not find Appellant's arguments persuasive since

Appellant's argument is not commensurate in scope with the language of independent claim 1. Specifically, Appellant argues that the information in the code of Dannhaeuser does not uniquely identify any particular one of multiple devices, but we do not find express support in the language of independent claim 1 to support this argument. Therefore, we do not find Appellant's argument persuasive.

Furthermore, the definition as provided in Appellant's Specification at page 5 merely states "'pseudonym' as used herein is intended to include device-identifying information transmitted by an RFID device, such as an identifier in a given set of multiple identifiers stored or generated in the device, or a portion of an identifier." Appellants' definition encompasses both stored and generated information which may identify the RFID device. We find no limitation express or implied in Appellant's definition that this value must be "unique" or that it must be stored or pre-existing. Therefore, we find the Examiner's combination of the teachings of Hughes in view of Dannhaeuser to be reasonable in light of the instant claim language as interpreted in light of Appellant's express definitions. Therefore, we find the Examiner's reliance upon the access challenge and response using the secret key and combination with pseudorandom numbers to identify or authenticate the RFID device as they generate pseudonyms since it provides some level of device identifying information. Therefore, we do not find Appellant's argument to be persuasive of the error.

Appellant argues that the remote keyless entry devices of Dannhaeuser would not be understood by one skilled in the art to constitute

RFID devices of the type recited in the claim at issue. (App. Br. 6). Appellant again argues that the RFID devices of the claimed invention allow the reader to uniquely identify the particular device with which it is communicating (App. Br. 6). Again, we find no support in the language of independent claim 1 for this argument, and do not find the argument persuasive.

Appellant argues that the RFID devices and remote keyless entry devices are entirely different types of devices, and one looking to improve an RFID device would generally not look to the remote keyless entry device art. Therefore, Appellant concludes that the teachings of Dannhaeuser are believed to represent non-analogous art relative to the teachings of Hughes. (App. Br. 6). We find that the Examiner has set forth a convincing line of reasoning for the combination of the multiple values as taught by Dannhaeuser to increase security in the wireless communication of Hughes as set forth at page 6 of the Answer. We do not find Appellant's general contention or belief to show error in the Examiner's line of reasoning. Therefore, we do not find Appellant's argument to show error in the Examiner's initial showing.

With respect to Appellant's argument concerning the Examiner's conclusory statements and a lack of objective evidence of motivation for the combination, Appellant argues that "such an arrangement would clearly be undesirable in an RFID system having a very large number of tags" (App. Br. 7). Again, Appellant's argument goes beyond the express limitations recited in independent claim 1. We find independent claim 1 merely recites

a minimum of a singular RFID device and a singular reader. Therefore, Appellant's arguments are not commensurate in scope with the instant claim language and cannot be persuasive of error.

Appellant additionally argues that it is believed that the Dannhaeuser technique is not only undesirable in an RFID system, but it is practically unworkable in such a system and contrary to the object is of Appellant's claimed invention in terms of providing techniques implementable in low-cost RFID devices with limited computational and storage resources. (App. Br. 7-8 and Reply Br. 5). Again, Appellant's arguments are not commensurate in scope with the instant claim language and cannot be persuasive of error.

Appellants additionally argue that the Examiner's combination is based upon piecemeal reconstruction and impermissible hindsight (App. Br. 8 and Reply Br. 3). We do not find Appellant's argument persuasive of error since the Examiner has set forth a reasoned argument on the record and Appellant has not shown error therein. In the Reply Brief, Appellant generally argues that the secret key value is not transmitted (Reply Br. 2-3). We agree with Appellant that the secret key value is not transmitted, but the Examiner relies upon the access challenge/response process. Therefore, Appellant's argument is not persuasive of error in the Examiner's initial showing.

Again, in the Reply Brief at pages 3-6, Appellant argues that the secret key value is not transmitted. As discussed above, we find the Examiner does not rely upon the transmission of the secret key value, but the

transmission of the value created using the secret key value in an access challenge and challenge response process. Therefore, Appellant's argument is not persuasive of error.

From our review of the teachings of Hughes and Dannhaeuser, we find that the combination teaches the invention as recited in independent claim 1. From our review of Appellant's arguments in the Brief and Reply Brief, we do not find that Appellant has shown error in the Examiner's prima facie case of obviousness over the combination of Hughes in view of Dannhaeuser with respect to independent claim 1.

Since Appellant has not shown error in the Examiner's initial showing, we will sustain the rejection of independent claim 1 and in dependent claims 2, 4, and 23-25 grouped therewith. Similarly, since Appellant has not set forth separate arguments for patentability with respect to independent claims 30 and 32, we will sustain the rejection of these claims.

Alternatively, we find that the teachings of Hughes, by itself, fully meet all the limitations of independent claim 1. We find that Hughes teaches associating a plurality of pseudonyms with the RFID device in the access challenge/response process using random number generation. Each time there is an access challenge/response a different response is generated for the different random number thereby associating a plurality of pseudonyms with the RFID device. We note independent claim 1 does not recite storage or maintaining of the pseudonyms at the RFID device.

Hughes teaches transmitting from the RFID device different ones of the pseudonyms in response to different reader queries from the RFID

device in the access challenge/response process where each challenge and response are different each time due to the different random numbers being used.

Hughes teaches the access challenge/response process where the reader verifies the identification of the RFID device. We note that independent claim 1 does not recite any temporal relationship between transmitting of the RFID device pseudonyms and queries. Here, we find that Hughes does teach transmitting pseudonyms in response to queries which are individual challenges and the corresponding responses from the RFID device.

As noted above, Hughes does teach all the limitations of independent claim 1. A disclosure that anticipates under 35 U.S.C. § 102 also renders the claim unpatentable under 35 U.S.C. § 103, for "anticipation is the epitome of obviousness." *Jones v. Hardy*, 727 F.2d 1524, 1529 (Fed. Cir. 1984). See also *In re Fracalossi*, 681 F.2d 792, 794 (CCPA 1982); *In re Pearson*, 494 F.2d 1399, 1402 (CCPA 1974). Thus, we sustain the Examiner's rejection of appealed independent claim 1 under 35 U.S.C. § 103.

With respect to dependent claims 5 and 6, Appellant argues that the relied upon portion of Hughes does not teach or suggest an authentication value unique to a given pseudonym as recited in the claims (App. Br. 8-9). We disagree with Appellant's and find that the cited portion of Hughes using random number access challenge values with encryption would have taught and fairly suggested the corresponding unique value. Therefore, we do not find that Appellant has shown error in the Examiner's rejection.

With respect to dependent claim 7, Appellant argues that the key values are not transmitted by the RFID device in Hughes and cannot be read on the claimed pseudonyms. As discussed above, we did not find this argument persuasive of error in the Examiner's initial showing, and we will sustain the rejection of dependent claim 7.

With respect to dependent claim 20, the Examiner identifies at page 7 of the Answer that figure 2 of Dannhaeuser teaches the storage of the same sequence of code words in both the transmitter and receiver. We do not find Appellant's generalized argument at page 9 of the Brief to show error in the Examiner's (corrected) citation to Dannhaeuser for support. Therefore, we will sustain the rejection of dependent claim 20.

With respect to independent claim 33, Appellant disputes the Examiner's treatment of independent claim 33 as similar in scope to independent claim 1 and argues that Dannhaeuser does not teach the claimed updatable set of one or more one-time pads (App. Br. 10). Appellant argues that Dannhaeuser makes no reference whatsoever to any aspect of cryptography, much less to one-time pads, as claimed. Here, we note the Examiner has further identified figure 3 of Hughes in addition to Dannhaeuser as supporting the proposition of utilizing an updatable set of one-time pads (Ans. 7). Appellant did not respond to the modified rejection by filing a Reply Brief. We agree with the Examiner and find that Hughes does teach and fairly suggest the use of cryptographic processing wherein each iteration with a different random number would generate an updated

response or "updatable set" of one (or more) values. Therefore, we do not find that Appellant has shown error in the Examiner's initial showing.

With respect to dependent claim 3, Appellant relies upon the arguments advanced with respect to independent claim 1 and asserts that the Turner reference fails to overcome the deficiencies in the combination of Hughes and Dannhaeuser. Since we did not find a deficiency in the base combination, we do not find Appellant's argument to be persuasive of error in the initial showing.

With respect to independent claim 31, Appellant disputes the Examiner's treatment of the scope of independent claim 31 as similar to independent claim 1 and dependent claim 3 (App. Br. 11). We agree with Appellant that the scope of claim 31 is different than independent claim 1 and dependent claim 3. With that said, Appellant's argument does not address the merits of the Examiner's rejection of independent claim 31 wherein the Examiner in the discussion of claim 3 discusses the teachings of Turner with respect to a plurality of readers and a plurality of RFID devices. Therefore, we find that the Examiner has made a proper initial showing with respect to the obviousness of independent claim 31. Therefore, we will sustain the rejection of independent claim 31.

With respect to dependent claims 9-16, Appellant relies upon the same arguments advanced with respect to independent claim 1 and asserts that Furuta fails to overcome the fundamental deficiencies of Hughes and Dannhaeuser (App. Br. 11). Since we did not find a deficiency in the base combination, we do not find Appellant's argument to be persuasive.

With respect to dependent claim 26, Appellant argues that the RFID device generates the plurality of pseudonyms as pseudonyms of a sequence of outputs or functions and that the collective teachings Furuta, Hughes, and Dannhaeuser do not meet the limitation in dependent claim 26 (App. Br. 12). We disagree with Appellant and find that Furuta teaches at column 8 a sequence of functions or an updatable rule. Therefore, we do not find that Appellant has shown error in the Examiner's initial showing, and we will sustain the rejection of dependent claim 26.

With respect to dependent claim 27, Appellant argues that the RFID device and the verifier of the system attempt to maintain a common counter unique to the RFID device and share the seed (App. Br. 12). Here, the Examiner merely repeats the limitation of the claim and cites to Hughes at column 5. From our review of column 5 of Hughes, we do not find an express teaching of a common counter and sharing a seed, as recited in dependent claim 27. Therefore, we agree with Appellant that the Examiner has not set forth a proper initial showing of the teachings or a convincing line of reasoning from the references applied. Therefore, we will reverse the rejection of dependent claim 27 and dependent claim 29 which depends therefrom.

CONCLUSION

In summary, we have sustained the rejection of claims 1-7, 9-16, 20, and 23-26 under 35 U.S.C. § 103(a), and we have reversed the rejection of claims 27 and 29 under 35 U.S.C. § 103(a).

No time period for taking any subsequent action in connection with this appeal may be extended under 37 CFR § 1.136(a).

AFFIRMED-IN-PART

pgc

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560